COUNCIL on FOREIGN RELATIONS

Summary Report

Cybersecurity, Foreign Policy, and Business

Washington, DC Workshop
January 11, 2011
8:00 a.m. – 3:00 p.m.

In early 2011, the Council on Foreign Relations held a workshop focused on the intersection of cybersecurity, foreign policy, and global business. The program, which included a keynote address by Philip Reitinger, Deputy Undersecretary of the National Protection and Programs Directorate at the U.S. Department of Homeland Security, consisted of three panels: supply chain security; balkanization of digital markets; and cyber exploits, private business, and national security. Participants included officials from the Departments of Commerce and Homeland Security as well as Senate and House staffers, industry representatives, and academic and policy analysts.

The central focus of the workshop was the potential for certain cybersecurity measures to balkanize the Internet and the overall global technology ecosystem. Today's relatively global, open, and interoperable digital infrastructure is being challenged by national spaces implementing competing technology standards and security processes. As more nation-states become concerned about cyber risk and seek to apply their own solutions, there has been a proliferation of constraints placed upon commercial technology companies—such as requests to examine proprietary source code—compliance with which would make it more difficult for them to operate globally. Some states seem to be working to undermine the current system of global technology security governance, which is currently marked by the participation of state actors, technology companies, and independent technical groups in relatively open, multi-actor fora, and replace it with a more closed, state-centric, sovereignty-oriented model.

The United States has a national interest in a global and open digital infrastructure. There are clear economic reasons for this. American technology firms have benefited from economies of scale and new models of global innovation. There are also strong national security arguments to be made: an open, transparent, and flexible system is likely to be more secure than one where national governments try to enforce multiple competing security standards.

While the United States government is well positioned to push a vision of a global digital infrastructure forward, it is not doing so as effectively as it could. If Washington does not lead on these issues, the impetus and energy for change may come from revisionist actors whose interest and values are not congruent with those of the United States.

Digital Infrastructure: Context

Almost every technology company relies on and must manage a global supply chain. This is true for the biggest companies with manufacturing and R&D locations around the world as well as smaller firms that source or deliver products through a supply chain that can span several countries and continents. While these networks bring real economic gains, they also bring the risks of greater interdependence. Software and hardware can be compromised at multiple points by numerous actors. Managing supply chains has become even more complex for suppliers, vendors, and customers, in part because these networks have become significantly more software- and services-based. This is a good thing for American companies as they "move up the stack" away from products that are rapidly becoming commodities, but also places greater demands on users as the rate of change is rapid. In effect, the risk is getting worse and there is unlikely to be a single set of engineering or technological solutions. Policymakers must try to envision the entire ecosystem in which suppliers, vendors, and customers cooperate and compete, realizing that any set of proscriptive solutions may create unexpected and unwanted outcomes.

Confronted with a similar set of security challenges, policymakers in Russia, China, India, the United States, Brazil, and elsewhere are responding with national laws or regulations that make multiple demands on technology firms dependent on location. The motivation for these demands is often opaque; policies can be driven by real security concerns, the desire to promote competing technology standards and strengthen domestic firms, or some combination of the two.

In the case of China, the objectives appear clearer. Policymakers in Beijing advocate a sovereignty-based model of the Internet that is tied to economic competiveness and national security. They are trying to shift discussions about the Internet's future out of multi-actor fora such as ICANN to the ITU and other international organizations where states wield greater power. In addition, China is using market access, procurement strategies, and other policies designed to encourage "indigenous innovation" to create new technology and security standards. On a positive note, as some Chinese firms are going global, they are beginning to look to the Common Criteria—an international security standard that is assured by national testing laboratories—as a way to enter markets and eventually these firms may be able to shape domestic cybersecurity policies.

It should be also noted that there is skepticism in the rest of the world about U.S. intentions. Some foreign governments see themselves and their networks as overly dependent on U.S. suppliers and fear that U.S. intelligence agencies have access to their networks. In many ministries and regulatory agencies around the world, it is widely assumed that there is a close relationship between U.S. firms and the National Security Agency.

Policy Process

In addressing this balkanization, there is some good news. Participants of the workshop pointed to a greater recognition of the issue—and their common interests—in industry and government. There was also a sense that industry and government largely shared a similar policy approach, one grounded, in the words of one of the participants, in the creation of the Internet itself. That is, the process should be open and developed in a global context by nongovernmental organizations. Public-private partnerships would figure prominently in U.S. strategy, with the private sector taking the lead supported by government policy. Or as one participant put it, "the power and authority of the U.S.

government combined with the much more knowledgeable technological expertise of the private sector."

While few questioned the strengths of this model, there was a sense that it needed to be energized and extended, especially as others pursued competing visions in more state-centric venues such as the ITU. Some of the apparent weaknesses of the open and decentralized model included the speed of decision-making within the government and the inability of traditional rule making processes to keep pace with technological and market change. As a reference, one participant noted that FCC Chairman Julius Genachowski recently reported that the average rule-making cycle is 6 years.

In addition, there was the larger issue of how to move from process to strategy. This was often referred to as a problem of coordination. Several public-private consultations may be going on at the same time; sometimes these processes may come together better than others. Since cybersecurity encompasses economic and national security issues, responsibilities are spread across numerous agencies or departments. The State Department, for example, has one bureau that deals with the ITU, APEC, and the OECD on economic and trade issues and another that addresses hacking and cyber intelligence issues through NATO and other organizations.

The appointment of Coordinator of Cyber Issues, announced in the 2010 Quadrennial Diplomacy and Development Review, should resolve some of the inevitable coordination problems that have emerged from such a decentralized approach. Indeed, the participants were clear: they were not looking for a "single plug-in" for all cyber issues. Still, there were concerns about what some saw as a lack of a comprehensive Internet foreign policy strategy, one that would empower policymakers to make decisions about tradeoffs and signal numerous agencies and departments about priorities and resource use. Without a comprehensive strategy, departments have different interpretations of their own and others' priorities and strategies. Moreover, a single vision makes it easier to engage both the private sector and U.S. allies and other potential international partners. As it stands now, these partners have to understand and interpret priorities and intentions on their own, drawing from multiple documents and voices.

Policy principles

Workshop participants identified several principles for moving forward on technology security:

1) **A Global Approach**. At the center of any policy response should be support for internationally recognized standards that enable consistent approaches to addressing technology security. This would be similar to the existing Common Criteria regime and a related broader effort, the Open Group Trusted Technology Forum that from the beginning is positioned to be an international partnership involving business and government.

2) **Global standards should underlie national approaches**. The standards do not stand alone, but are part of a flexible regulatory model that encompasses multiple actors across various ecosystems. One participant suggested the food safety system as a possible analogy, highlighting the importance of independent oversight primarily maintained by industry participants but also with government intervention as well.

3) **Government policy should be technology-neutral and outcome-oriented**. The right mix of market-based incentives and government regulations needed to raise the floor on security is, of course, crucial. The majority of workshop participants supported a private-sector led solution, where the government provides encouragement, support, and in some instances creates incentives for private action. In these instances, the government's focus should be on outcomes, not specific technological means.

4) **Beware the consequences of unilateral action**. Moving forward, policymakers must keep in mind the impact that U.S. government actions have on other actors. If the U.S. insists on developing its own domestic standards, then it cannot expect Russia, Brazil, China, or others not to pursue the same remedy.

5) **Pursue strategic alliances**. Given international skepticism about U.S. intentions in cyberspace, policymakers need to find the right partners with which to pursue these policies and, in some instances, encourage them to take the lead. Examples might include Australia in Asia-Pacific Economic Cooperation (APEC), Brazil in the Organization of American States (OAS), and India given its increasing global influence.

Cyber espionage, national security, and economic security

During the afternoon, workshop participants turned their attention to the issue of attacks on U.S. corporations. In the September 2010 issue of *Foreign Affairs*, Deputy Secretary of Defense William Lynn III argued that though the "threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyber threat that the United States will face over the long term."

Since Lynn's article appeared, public reports have indicated that DuPont, Johnson & Johnson, General Electric, RSA, and at least a dozen others have had proprietary information stolen by hackers. Given the scope of the threat, should the United States government have a greater role in combating corporate espionage and intellectual property theft? If so, should one agency take the lead? How should the government sector and private industry work collaboratively to defend against attacks?

In contrast to the morning session, there were some sharper differences in defining the problem. While the attacks on the intellectual property of companies could traditionally be conceived of as a law enforcement problem, the fact that many of the attacks are launched from other countries means that they also become foreign policy and national security challenges. Moreover, as one participant argued, criminal prosecutions do not serve as an effective deterrent. Countries such as Russia rarely cooperate with U.S. requests to prosecute hackers.

Most notable, some participants, especially in contrast to the discussion on supply chain security, made a more forceful argument for greater government regulation in the face of a market failure. In this instance, the Internet's culture of decentralization and deregulation, while critical to continued innovation, is failing to address a serious security threat that is only worsening. The obvious challenge, if greater regulation is indeed the answer, is how to set guidelines without losing the good side of deregulation. Can the government move the market enough through incentives, procurement policy, and support of R&D or is more direct intervention required?

Given the attacks on Google and others, there was skepticism that even the biggest companies would be very successful on their own against state or state-backed hackers. Or as one participant put it, the private sector has the expertise to deal with "geek versus geek attacks" but not "spy versus spy." Those skills were to be found in the National Security Agency. In this environment, the objective for the private sector is risk management, with the government and U.S. Cyber Command playing defensive and deterrent roles, respectively.

Despite the centrality of information sharing to public-private partnerships, participants noted the failure to develop a mechanism to ensure that the government shares information in a timely and relevant manner. While the finance and communication sectors in particular are thought to allow for relatively effective sharing through the Information Sharing and Analysis Centers, one participant referred to a case where the government knew of an attack on a telecommunications company four months before the company knew. From the other side, government representatives spoke of the private sectors' unwillingness to disclose information about security breaches out of fear that the admissions would spark questions from investors and regulators.

Through the Defense Industrial Base Information Sharing Environment, forty defense contractors share information on attacks in return for Department of Defense assistance with network defense. Recent reports suggest that the Pentagon will offer to develop a similar program for Internet service providers. In addition, the newly opened National Cybersecurity and Communications Integration Center (NCCIC) is expected to collocate government and industry representatives to allow for coordinated planning and response. Yet, it is clear that without common knowledge and shared understandings it will be impossible to create the consensus needed for clear policy.

As with the discussion on supply chain security, there was a widely shared sense that greater policy clarity was needed. There were questions of whether repeating the need for public-private cooperation and information sharing was enough; these date back to at least 1995 or 1996 and no one doubts that the United States is still not moving fast enough. Rather than simply repeat these mantras, the restated policy would more clearly define roles and responsibilities, both within the government and between the government and private sector.

Moving forward

The workshop's discussions point to the need for a coherent Internet foreign policy. While the United States' economic and soft powers are important strengths, a more proactive strategy is necessary in the pursuit of national interests. This strategy would not only make it more likely that separate agencies work together but would also provide a policy framework for balancing the tradeoff among the economic, security, and governance issues that are part and parcel of the United States' presence in cyberspace.

The emergence of such a unified policy was seen to be the likely outcome of two possible events: a catastrophic attack, or the exercise of high level leadership. Since all want to avoid the first catalyst, and suspect that decisions made soon after a crisis are likely to get the balance among security, economic, and privacy issues wrong, we hope that over the next year or two, leaders in the public and

private sector will begin to craft a coherent picture of where the United States needs to go and how it will get there.

The Council on Foreign Relations gratefully acknowledges IBM and Thomson Reuters for their support of this workshop.